Runtime randomization and perturbation for virtual machines.

JAVIER CABRERA ARTEAGA

Licentiate Thesis in [Research Subject - as it is in your ISP]
School of Information and Communication Technology
KTH Royal Institute of Technology
Stockholm, Sweden [2022]

KTH School of Information and
Communication Technology
SE-164 40 Kista
SWEDEN

TRITA-ICT XXXX:XX
ISBN XXX-XX-XXXX-XXX-X

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges till offentlig granskning för avläggande av licentiatexamen i [ämne/subject] [veckodag/weekday] den [dag/day] [månad/month] [år/2022] klockan [tid/time] i [sal/hall], Electrum, Kungl Tekniska högskolan, Kistagången 16, Kista.

© Javier Cabrera Arteaga, [month] [2022]

Tryck: Universitetsservice US AB

Abstract

Write your abstract here...
Keywords: Keyword1, keyword2, ...

Sammanfattning

Write your Swedish summary (popular description) here...
Keywords: Keyword1, keyword2, ...

Acknowledgements

Write your professional acknowledgements here...

Acknowledgements are used to thank all persons who have helped in carrying out the research and to the research organizations/institutions and/or companies for funding the research.

Name Surname,
Place, Date

Contents

Contents **vi**

List of Figures **viii**

List of Tables **ix**

List of Acronyms **x**

1 Variant's generation **1**

1.1 CROW . . . 1

1.1.1 Example . . . 3

1.2 Evaluation . . . 4

1.2.1 Corpora . . . 5

1.2.2 Setup . . . 5

1.3 Results . . . 6

1.3.1 Challenges for automatic diversification . . . 7

1.3.2 Properties for large diversification using CROW . . . 8

1.3.3 Variant properties . . . 8

1.4 Conclusions . . . 9

2 Variant's assessment **10**

2.1 Metrics . . . 10

2.1.1 Static . . . 10

2.1.2 Program traces and execution times . . . 11

2.1.3 Variants preservation . . . 11

2.2 Evaluation . . . 12

2.3 Results . . . 13

2.3.1 Static . . . 13

2.3.2 Dynamic . . . 13

2.3.3 Preservation . . . 13

2.4 Conclusions . . . 13

3 Variants Usage (CROW + MEWE) **14**

3.1 Security MTD 14
3.2 Reliability (CVE + fuzz) future work 14

Appended papers **14**

List of Figures

1.1 CROW workflow to generate program variants. CROW takes C/C++ source codes or LLVM bitcodes to look for code blocks that can be replaced by semantically equivalent code and generates program variants by combining them. 2

List of Tables

1.1 Corpora description. The table is composed by the name of the corpus, the selection criteria and the stats the programs in each corpus. 6

1.2 CROW tweaking for variants generation. The table is composed by the name of the corpus, the timeout parameter and the maximum number of instructions allowed in the synthesis process. 6

1.3 General diversification results. The table is composed by the name of the corpus, the number of functions, the number of succesfully diversified functions, the number of non-diversified functions and the number of unique variants. 7

2.1 Wasm engines used during the diversification assessment study. The table is composed by the name of the engine and the description of the compilation process for them. 13

List of Acronyms

Wasm	WebAssembly
DTW	Dynamic Time Warping